TØI-rapport 914/2007
Forfattere: Torkel Bjørnskau, Mattias Gripsrud,
Tonje Grunnan, Tore Leite, Dag Wiese Schartum
Oslo 2007, 108 sider

Sammendrag:

Security i transport og personvernets grenser

Intensivert security etter 11. september 2001

Særlig i luftfart og sjøfart er det innført en rekke nye bestemmelser og tiltak som følge av terrorangrepene i USA 11. september 2001. Også terroraksjonene mot jernbanen i Madrid i 2004 og mot kollektivtrafikken i London i 2005 samt avsløringene av planlagte terrorangrep mot transatlantiske flygninger sommeren 2006 har gitt økt fokus på terrorsikring og vært bakgrunnen for nye tiltak. Noen av de viktigste tiltakene som er innført er:

- Intensivert security-sjekk av passasjerer og bagasje på internasjonale og nasjonale lufthavner
- Innføring av biometriske pass. Krav om biometriske pass for innreise til USA
- Utlevering av passasjerlister med personopplysninger fra flyselskapene til amerikanske myndigheter
- Forbudet mot å bringe væskebeholdere med over 1 dl væske om bord i fly
- Kroppsskannere for å undersøke passasjerer er innført som forsøksordning bl.a. på Schiphol lufthavn i Amsterdam
- Fingeravtrykkavleser som sikrer samsvar mellom person som sjekker inn bagasje og som går om bord i fly er innført av SASBraathens på Oslo Lufthavn
- Strengere krav til sikkerhet og terrorberedskap for skip, bl.a. terroralarm, besiktigelse og kontroll av skip, krav til sikringsplaner, sikkerhetsutstyr mv.
- Strengere regler for fysisk sikring av havneområder, med inngjerding, adgangskontroll mv.
- Strengere krav til identifikasjonsbevis for sjøfolk
- Strengere kontroll av hvem som ansattes i transportvirksomhet (kontroll av bakgrunn og vandel)
- Fysisk kontroll av containere, skanningsteknologi, utvikling av ”smarte” containere, radiofrekvensidentifikasjon, satellittbaserte sporingssystemer mv.
- Forsøk med passasjerkontroll på utvalgte T-banestasjoner på undergrunnen i London

Rapporten kan bestilles fra:
Transportøkonomisk institutt, Gaustadalleén 21, NO 0349 Oslo
Telefon: 22 57 38 00 Telefax: 22 60 92 00

Som det framgår av denne listen er det særlig i luftfart og sjøfart at security-arbeidet er intensivert. Dette er transportgrener der security har vært nokså sterkt fokusert også tidligere. Det ser m.a.o. ut til at den nye terrortrusselen først og fremst har ført til nye tiltak på områder der det allerede er et visst securityregime fra før, og i langt mindre grad at det er kommet securitytiltak på helt nye områder.

Det finnes imidlertid en rekke tiltak innenfor alle transportgrener som ikke har terrorsikring som primært formål, men som innebærer overvåking og registrering av personer/kjøretøy og som dermed har personvernimplikasjoner og som har vært brukt eller kan brukes til forebygging/oppklaring av terroraksjoner eller -planer.

Dette gjelder kameraovervåkning av terminaler, transportmidler, infrastruktur og stasjonsområder som særlig er utbredt i Storbritannia, men som også er blitt stadig mer vanlig i Norge. Videre finnes det automatiske systemer for å registrere kjøretøyers passeringer i bomstasjoner (AutoPass), elektroniske billetteringssystemer, automatiske satellittbaserte fartstilpasningssystemer (”Intelligent speed adaptatation” (ISA)) og systemer for automatisk varsling av ulykker (e-call), atferdsregistrator (”black box”) i bil, automatisk trafikkontroll. Dette er systemer som enten er innført eller som er på trappene og som innebærer overvåkning og registrering av personopplysninger. Særlig innenfor veitransport skjer det en voldsom utvikling når det gjelder å ta i bruk ny teknologi for å styre og overvåke trafikken.

Slike systemer har åpenbare implikasjoner for personvern – og dels av samme grunn – kan de utnyttes i arbeidet mot terror. Det britiske systemet med automatisk registrering av kjennemerker på passerende biler (”Automatic Plate Number Recgonition” (APNR)) ble for eksempel brukt til å spore opp en av de terrormistenkte bak bilbombeaksjonene i London og Glasgow sommeren 2006.

Terrorsikring i norsk transport – tilpasning til internasjonale avtaler

Terrorsikring i norske transportvirksomheter skjer nær sagt utelukkende ut fra internasjonale forpliktelser. Luftfart og sjøfart er de transportgrenene hvor det tradisjonelt har vært et omfattende internasjonalt regelverk gjennom ICAO, IMO og etter hvert EU, og det er også i disse transportgrenene at de fleste sikringstiltak mot terror er implementert i Norge, som i de fleste andre vestlige land.

Det er få selvstendige initiativ når det gjelder tiltak mot terror mot transportmidler eller infrastruktur i Norge. Det innføres riktignok securitytiltak i alle de fire transportgrenene ut fra egne initiativ, men disse er begrunnet ut fra ønsker om å forhindre vanlig kriminalitet som tagging, hærverk og vold.

To hovedprinsipper for terrorsikring

Sikring mot terrorhandlinger kan i prinsippet skje på to ulike måter. For det første kan man forsøke å sikre utvalgte objekter slik at potensielle terrorister enten avskrekkes fra å forsøke å angripe, eller slik at de vil bli avslørt før de får gjennomført angrepet. Dette har vært hovedprinsippet for sikring i luftfarten; alle

personer og all bagasje som skal om bord i fly må gå gjennom streng sikkerhetssjekk for å sikre at ulovlige og potensielt skadelig gjenstander ikke bringes om bord. Det innebærer imidlertid at også pilotene må gjennom sikkerhetskontrollen.

For det andre kan man forsøke å sikre seg gjennom spaning og overvåkning av potensielle terrorgrupper slik at man kan pågripe dem før de får anledning til å gjennomføre et angrep. En slik strategi basert på politimetoder, spaning, registrering og etterretning dreier seg ikke om å sikre bestemte objekter, men å slå til mot potensielle terrorister før de aksjonerer, uavhengig av hva slags mål de måtte ha for en aksjon.

Konflikt mellom personvern og terrorsikring

Begrepet personvern er knyttet til demokratiske verdier som rettssikkerhet og borgerrettigheter, blant annet retten til en privatsfære og til personlig integritet. Retten til personvern er nedfelt i Den europeiske menneskerettighetskonvensjonen av 1950 og i EUs personverndirektiv.

Personvern kan noe forenklet sies å bestå av vern av personers *integritet* og vern av *opplysninger* om enkeltpersoner. Integritetsvern tilsvarer det engelske begrepet *privacy protection*, mens opplysningsvern tilsvarer begrepet *data protection*.

Opprinnelig var begrepet personvern i stor grad assosiert med integritetsvern dvs. vern mot innsyn i privatlivet/privatsfæren. Etter hvert som elektroniske datalagringssystemer ble utbredt utover på 1970-tallet ble begrepet personvern i økende grad brukt i betydningen personopplysingsvern, dvs. i forhold til innsamling, registrering og bruk av personopplysninger i elektroniske systemer.

Objektkontroll utfordrer primært integritetsvernet

Begge strategier for sikring mot terror som er beskrevet har personvernimplikasjoner, men på forskjellige måter. Sikring av objekter gjennom passasjerskanning og lignende har først og fremst implikasjoner for integritetsvernet. Fysisk kontroll av passasjerer skal sikre ingen bringer inn ulovlige og farlige objekter. Kontrollen gjelder uansett, og det spiller i prinsippet ingen rolle hvem personen er. Objektkontroll er derfor i utgangspunkt uavhengig av personregistre og personopplysninger, og utfordrer dermed heller ikke personvernet i betydningen personopplysningsvernet.

Forebygging av terror utfordrer primært opplysningsvernet

Motsatt gjelder for forebyggingsstrategien som innebærer overvåkning og registrering av enkeltpersoner og grupper som av en eller annen grunn kan mistenkes for å utgjøre en terrortrussel. Det ligger i sakens natur at en slik strategi baseres på at man må samle inn og lagre en stor mengde opplysninger om en rekke personer som så danner grunnlag for eventuell tettere oppfølging gjennom spaning, avlytting osv. Denne strategien utfordrer dermed først og fremst personopplysningsvernet i og med at en mengde opplysninger om enkeltpersoner

innhentes og lagres. Strategien utfordrer også integritetsvernet, men først og fremst når det gjelder personer som blir underkastet detaljert oppfølging i form av avlytting osv. Folk som ikke blir fulgt opp slik opplever trolig i liten grad at registrerings- og overvåkningssystemer strider mot integritetsvernet.

I den grad objektkontrollen skjer ved hjelp av elektronisk apparatur eller det på annen måte registreres opplysninger med utgangspunkt i slik kontroll, er det grunn til å se integritetsvern og opplysningsvern i sammenheng. Bruk av biometriske metoder og forsøk med kroppsskannere tyder på at en slik sammenkopling av de to aspektene ved personvernet kan bli stadig viktigere.

Avveining mellom personvern og sikring

Personverninteressene

Personvernspørsmål blir i faglitteraturen ofte diskutert med referanse til den såkalte "interesseteorien". Denne teorien er et forsøk på å systematisere og konkretisere hva som skal forstås med personvern. I følge interesseteorien består personvernet av en rekke "enkelt-interesser" som til sammen kan antas å representere våre interesser når det gjelder personvern. I følge interesseteorien har vi følgende hovedkategorier av interesser knyttet til personvernet:

a) Interesse i å bestemme over opplysninger om egen person

b) Interesse i innsyn og kunnskap

c) Interesse i opplysnings- og behandlingskvalitet

d) Interesse i forholdsmessig kontroll

e) Interesse i brukervennlig behandling

f) Interesse i personvernanalyse

Punkt (a) innebærer at man ønsker å bestemme hvilke opplysninger om egen person som skal lagres og være tilgjengelig for myndigheter og andre. I svært mange sammenhenger ivaretas denne interessen av kravet om at individer må samtykke i at opplysninger om dem blir registrert. Punkt (b) innebærer at man skal ha innsyn og kunnskap om hvilke opplysninger om egen person som er registrert. Punkt (c) innebærer at man er interessert i at det ikke er ukorrekte opplysninger som er lagret, og at eventuelle feil blir rettet. Punkt (d) dreier seg blant annet om at det må være en forholdsmessighet mellom graden av informasjon om egen person som registreres og det formål opplysningene innhentes for. Det kan også dreie seg om at en form for kontroll skal nøye vurderes i forhold til andre mulige kontrollformer. Punkt (e) om interesse i brukervennlig behandling, innebærer at informasjon om registre, lagringsprosedyrer osv. skal være lett tilgjengelig og at reglene som regulerer dette skal være forståelige.

Punkt (f) "Interesse i personvernanalyse" er føyet til i denne framstillingen som en presisering av interesseteorien, med spesiell relevans for securitytiltak i transport. Dette dreier seg om at hensynet til personvernet skal være nøye vurdert når ulike tiltak, som for eksempel securitytiltak i transportsektoren planlegges og

implementeres. Det innebærer for eksempel at ordinære krav til utredning av konsekvenser bør gjennomføres ved implementering av securitytiltak, at tiltakene skal være underlagt løpende kontroll, og at slike tiltak bør evalueres både med hensyn til effekt og kost/nytte, både på individ- og samfunnsnivå.

Terrorsikring truer personverninteressene

Det er nokså innlysende at alle punktene (a)-(f) i mange tilfeller ikke oppfylles når det gjelder securitytiltak. Som nevnt vil særlig overvåkningsstrategien måtte innebære hemmelig registrering av personopplysninger. Det innebærer registrering uten samtykke og med svært begrensete muligheter for å få innsyn i hvilke opplysninger som er registrert om egen person. Det innebærer også at interessen i opplysnings- og behandlingskvalitet rammes. Dersom enkeltpersoner ikke selv får anledning til å kontrollere hvilke opplysninger om dem som er registrert, vil mulighetene for å rette opp feil også bli svært mye dårligere.

Vilkårene for å imøtekomme interessen i forholdsmessig kontroll blir også nokså magre når hver enkelt ikke vet hvilke opplysninger som er registrert. Når formålet med overvåkning er å forebygge mulige terroraksjoner, blir også behovet for informasjon åpent; det er nesten umulig på forhånd å vite hvilken informasjon som vil være relevant. Da blir det også omtrent umulig å bestemme om informasjonsinnhentingen står i et balansert forhold til formålet.

Brukervennlig behandling er også svært vanskelig å imøtekomme når det gjelder securitytiltak. Som nevnt er det meste av som skjer på denne fronten i Norge implementering av internasjonale bestemmelser. For eksempel er de internasjonale reglene når det gjelder forebygging av anslag mot sikkerhet i luftfarten nedfelt i en egen forskrift til luftfartsloven. Denne forskriften peker til fem EU-forordninger og gir supplerende bestemmelser til disse. Flere av disse forordningene er blitt endret en rekke ganger, samtidig som flere av dem har vedlegg som er klassifiserte og unndratt offentligheten.

Hemmelighold og begrensede innsynsrettigheter bryter på grunnleggende måter med den ideologi som ellers har vært lagt til grunn på personvernområdet. Det som trer inn i stedet er en forhåpning om at myndigheter og ulike kontrollaktører opptrer innenfor rammene av grunnleggende menneskerettigheter og i samsvar med gjeldende nasjonale rettsregler. Tillit uten grunnlag for å etterprøve tilliten på grunn av hemmelighold er imidlertid problematisk i en demokratisk rettsstat.

Gjennomgangen av interesseteorien viser at tiltakene som iverksettes mot mulige terrorangrep både i transportsektoren og på andre områder, omtrent uten unntak kommer i konflikt med prinsippene om personvern. Det er imidlertid til en viss grad mulig å kompensere for dette gjennom forsterkede rettssikkerhetsgarantier.

Mye av rettsreguleringen når det gjelder personvern og sikring er prosedyreorientert til forskjell fra misbruksorientert. Det betyr at lovgivningen som for eksempel personverndirektivet, angir hvilke framgangsmåter som skal følges. En detaljert konkretisering av for eksempel hvilke personopplysninger som kan innhentes, brukes og registreres i tilknytning til kontroll av personer i for eksempel transportsektoren, vil gjøre kontrollen mer forutsigbar og mer etterprøvbar, og slik sett blir kontrollregimet mer akseptabelt i forhold til personvernhensyn og rettssikkerhet.

Et annet aspekt ved en slik prosedyreorientert tilnærming innebærer å ta i bruk teknologi og metoder som i størst mulig grad anonymiserer eller pseudonymiserer kontrollobjektene. Sikkerhetskontroll bør med andre ord i størst mulig grad skje uten at personers (virkelige) identitet avsløres. Ut fra hensynet til personvern kan maskinell tilgang til personopplysninger være å foretrekke framfor manuell tilgang. Årsaken er at personvernet kan sies å være mest krenket når personopplysninger kommer til menneskers kunnskap.

Det ligger i sakens natur at tiltak mot terror dels må baseres på hemmelig overvåkning og registrering. For å kompensere for dette kan man stille skjerpede regler både til framgangsmåte, behandling og lagring av slike opplysninger. Det kan for eksempel tenkes forbud mot at transportselskaper innhenter og bruker opplysninger i vandelsattester som er eldre enn fem år; krav om at visse minimumsbetingelser når det gjelder identifisering og autentisering må være oppfylt for å kunne legge noe frem som en personopplysning i en sak; rett til å få uavhengig sakkyndig granskning av informasjonssystemer som har generert ufordelaktige personopplysninger og klarlegging av straffeansvar for ulovlig innhenting og bruka av personopplysninger.

Norske transportaktørers syn på sikring og personvern

Representanter fra de fire transportgrenene samt fra relevante myndighetsorganer ble stilt en rekke spørsmål om securitytiltak som er gjennomført i ulike virksomheter. Det ble spurt om personvernimplikasjoner av securitytiltakene, om hvordan hensyn til personvern og security balanseres og hvordan arbeidet med security er forankret i organisasjonen.

Representanter fra følgende instanser/virksomheter ble intevjuet: Oslo T-banedrift, Oslo Havn, E18 Bjørvika, Datatilsynet, Nasjonal sikkerhetsmyndighet, Kystdirektoratet, Jernbaneverket, NSB, Luftfartstilsynet og Vegdirektoratet.

Særtrekk ved transportgrenene bestemmer security-nivået

Respondentene ga klart uttrykk for at særtrekk ved de ulike transportgrenene har avgjørende betydning for hvor mye fokus en har på terrorsikring. Et moment som ble trukket fram er at massetransportmidler i storbyområder har så mange passasjerer, avganger og holdeplasser at det er praktisk umulig å innføre et securityregime slik man har i luftfart. Også de rene bedriftsøkonomiske kostnadene ved dette vil være langt større enn hva man kan klare.

Det er også avgjørende forskjeller mellom transportnettverkene som de ulike transportgrenene opererer i. Luftfart er kjennetegnet av sentralisert punkt-til-punkt trafikk, der lufthavnene er plassert utenfor øvrige knutepunkter og dermed lettere å skjerme rent fysisk enn for eksempel jernbane og T-bane. Veitrafikk kjennetegnes ved en eksterm grad av åpenhet og det er omtrent umulig å tenke seg adgangskontroll for å delta i veitrafikken.

Et annet og beslektet element dreier seg om hvor integrert transportsystemene er med øvrig samfunnsliv og hverdagsliv. At hyppige trikkeavganger gis betegnelsen ”rullende fortau” illustrerer hvordan trikk (buss og T-bane) oppleves som en

integrert del av bysamfunnet. Massiv sikkerhetssjekk av passasjerer oppleves som uforenlig med et levende bysamfunn.

Flere informanter peker også på at det er store forskjeller i risikoaksept mellom transportgrener. Luftfart skiller seg ut med ekstremt lav risikoaksept og med tilsvarende høye security-kostnader. Flere peker på at sikkerheten for samfunnet som helhet ville øke om man flyttet ressurser fra securitytiltak i luftfarten over til ordinære trafikksikkerhetstiltak i veisektoren.

Mange peker også på at de forskjellige transportgrenenes institusjonelle forankring og regelverk i stor grad påvirker hvilket spillerom virksomhetene i de ulike transportgrenene har i valg og utforming av security-tiltak. Særlig sjøfart og luftfart er kjennetegnet av at de enkelte virksomheter må implementere internasjonalt regelverk.

Personvernimplikasjoner for egne ansatte og for trafikanter

Aktørene har ulike oppfatninger både når det gjelder *om* tiltakene de har gjennomført har personvernimplikasjoner og *hvem* de har implikasjoner for. Særlig i veisektoren oppleves personvernspørsmål i større grad å være en aktuell problemstilling når det gjelder egne ansatte enn når det gjelder trafikantene. I luftfart er oppfatningen at det er passasjerenes personvern som berøres av security-tiltakene.

Datatilsynet opplever at man i luftfart er svært bevisst spørsmål om personvernimplikasjoner av ulike tiltak, men at dette ikke gjelder i de andre transportgrenene. I luftfart er det særlig sikkerhetskontrollen av passasjerer som har personvernimplikasjoner. T-banen gir uttrykk for at de tradisjonelt er meget forsiktige når det gjelder tiltak med personvernimplikasjoner og at de følger myndighetenes krav. For Oslo Havn er hovedfokus å innføre internasjonale bestemmelser når det gjelder sikring, og personvern er ikke spesielt fokusert. Statens vegvesen er først og fremst opptatt av personvernspørsmål knyttet til trafikksikkerhetstiltak som innebærer overvåkning, og da særlig såkalt ”streknings-ATK”. I arbeidet med senketunnelen i Bjørvika i Oslo er det innført adgangskontroll og andre sikringstiltak, men personvernspørsmål har fått lite oppmerksomhet. Jernbaneverket forvalter infrastruktur og er i den forbindelse i liten grad involvert i spørsmål med personvernimplikasjoner, men opplever at slike spørsmål er relevante når det gjelder egne ansatte i forbindelse med sikkerhetsklarering av medarbeidere. NSB er klar over personvernimplikasjonene av kameraovervåkning og har bevisst valgt teknologi og prosedyrer for å minimere personvernimplikasjonene. Også i NSB er personvernspørsmål i stor grad rettet mot vern av ansatte.

Det generelle inntrykket er at personvern ikke er gjenstand for stor oppmerksomhet i norske transportvirksomheter, men at de ulike aktørene har vurdert personvernimplikasjoner av tiltak i egen virksomhet. Ingen mente at avveining mellom personvern og security var noe stort problemområde. Datatilsynet har stanset en del tiltak, men dette har i første rekke vært tiltak som har hatt andre formål enn terrorsikring.

Oppfatninger av security og safety i dag og i framtiden

Distinksjonen mellom safety og security er kjent i norske transportvirksomheter. Mange inkluderer sikring mot ordinær kriminalitet som hærverk, tagging, tyveri osv. i security-begrepet. Mange opplever også at det er tett sammenheng mellom safety og security; securitytiltak kan ha positive sideeffekter for safety. I forbindelse med beredskapsplaner oppleves distinksjonen safety/security som lite hensiktsmessig. Hvis en brann bryter ut må man ha beredskap til evakuering/slokking uavhengig av hva årsaken til brannen er.

De viktigste security-tiltakene med implikasjoner for personvern som er gjennomført blant norske transportvirksomheter er: kameraovervåkning av transportmidler og infrastruktur, informasjonstiltak og opplæring, adgangskontroll for passasjerer og ansatte og inspeksjoner og fysisk sikring av transportmidler og infrastruktur. Alle nevner også nær kontakt med politiet gjennom PST. Avanserte overvåkningssystemer som automatisk ansiktsgjenkjennelse, avanserte røntgenløsninger osv. ble opplevd som lite relevante, bortsett fra i luftfart der løsninger basert på biometri trekkes fram.

Organisatorisk er security plassert i tradisjonelle safety-avdelinger i T-banen, i Jernbaneverket, i NSB og Vegdirektoratet. Også i Kystdirektoratet og i havnevesenet er security og safety integrert i de samme enhetene. I Luftfartstilsynet er imidlertid dette delt der en egen avdeling arbeider med security, atskilt fra safety-spørsmål.

Alle transportgrenene arbeider systematisk med sikkerhetsspørsmål blant annet gjennom å utarbeide Risiko- og sårbarhetsanalyser (ROS). Terrortrusselen inngår som en del av trusselbildet. Tiltak mot terrortrusselen har som positiv sideeffekt at også ordinær kriminalitet blir redusert.

De fleste aktørene ser et behov for bedre koordinering av securitytiltak mellom transportgrener, men ikke behov for et felles regelverk på security-feltet. De fleste mener overvåkningen vil tilta i årene som kommer, men ser ikke for seg at ”flyplasslignende tilstander” vil komme i andre transportgrener, bortsett fra når det gjelder sjøtransport/havnesikring.

Security, effektivitet og rettssikkerhet

Det er begrenset fokus på terror og personvern i norsk transport. Det meste av terrorsikringen skjer som følge av internasjonale forpliktelser, og det er i de transportgrenene som tradisjonelt har vært regulert gjennom internasjonale avtaler – luftfart og sjøfart – hvor også security-tiltakene er innskjerpet og utvidet de senere år. Sikkerhetssjekken på flyplasser er for eksempel blitt betydelig skjerpet.

Ansvaret for security-tiltak er i stor grad organisasjonsmessig plassert i de samme enhetene som har ansvaret for ordinære sikkerhetstiltak (safety), og det er i stor grad den samme type hendelsesbaserte sikkerhetstenkningen som benyttes i utformingen av tiltakt mot terror. Det innebærer imidlertid at man overser at terroraksjoner gjennomføres at personer som tilpasser angrepet til de sikringstiltakene som gjennomføres, og som vil velge å angripe der man minst venter det. Det innebærer igjen at hendelsesbasert sikkerhetstenkning er av svært

begrenset relevans når man står overfor mulige terroraksjoner. Og det betyr at ytterligere sikring av objekter som alt er godt sikret ikke har særlig effekt.

Fra et samfunnsmessig synspunkt virker det nokså åpenbart at det ikke er en rasjonell balanse mellom tiltakene som settes i verk i luftfarten og mangelen på tiltak i andre transportgrener. Det fremstår i dag som litt av et tankekors at man ikke kan ta med vannflasker om bord i fly, mens det ikke foregår noen som helst kontroll passasjerer eller bagasje på tog og T-bane.

Objektsikring er derfor i beste fall ”lokalt” rasjonelt og kan bidra til å flytte risikoen til andre objekter som er dårligere sikret. For samfunnet vil imidlertid en strategi basert på objektsikring både være kostbar og lite effektiv. For mange transportvirksomheter – særlig veitrafikk og kollektivtransport i storbyene – er det ikke mulig å sikre seg mot terrorangrep gjennom tradisjonelle objektsikringstiltak. Erfaringer fra andre land viser også at i den grad man har lyktes i antiterrorarbeidet, så er det særlig gjennom forebygging av terrorangrep gjennom spaning og overvåkning at dette har skjedd.

Sikkerhetssjekk for å sikre bestemte områder eller objekter, slik man har i sikkerhetssjekken på flyplasser, har klare implikasjoner for personvernet i betydningen integritetsvern. Kroppsskanning og kroppsvisitasjon vil lett oppleves som inngrep i den enkeltes private sfære. Terrorsikring gjennom overvåkning og registrering av mistenkelige personer vil imidlertid kunne ha enda mer alvorlige konsekvenser for personvernet. Ikke bare vil slik overvåkning og registrering kunne omfatte veldig mange personer, registrering av informasjon innebærer også lagring i databaser med en rekke muligheter for å kobling av informasjon, for lekkasjer, for feilregistreringer mv. Fordi objektsikring bare er realistisk å gjennomføre innen luftfart og sjøfart, kan omfattende overvåking og registrering tenkes som strategi for å kompensere for manglende kontroll med reisende på tog, T-bane og buss mv. Et slikt valg vil ha store og alvorlige implikasjoner for personvernet.

Dersom vi gir kontrollører vide fullmakter til å gjennomføre kontroller som krenker personvernet, oppstår det også viktige spørsmål vedrørende tilstrekkelig kontroll med kontrollørene. Det er lett å tenke seg at det vil kunne utvikle seg egeninteresser knyttet til trusselnivået som vil være spesielt problematiske fordi det i stor grad er de samme enhetene som til enhver tid bestemmer trusselnivået, som også får tilført ekstra ressurser når trusselnivået øker. Det er godt mulig at dette til nå ikke har vært noe problem, men uansett er konstellasjonen uheldig; det er lett å mistenke at for eksempel sikkerhetstjenesten kan se seg tjent med å gi uttrykk for at terrortrusselen er høyere enn den faktisk er.

Dette er ikke bare utfordringer for personvernet, men for hele vår demokratiske rettstradisjon. Hemmelig politi med utvidete fullmakter og monopol på informasjon om trusler er noe vi ikke assosierer med rettsstaten. Spørsmålet som må stilles er om truslene vi står overfor kan forsvare slike brudd på demokratiske rettsstatsprinsipper.